Policy Title	Information Systems Acceptable Use Policy
Document identifier	PPM/ICT-ACCEPTABLE-USE/2024
Previous title (if any)	N/A
Policy objective	This policy has been written to define the proper use of information technology and related resources and data, and to ensure the security and technical integrity of the system. Inappropriate use of ICT assets exposes UNFPA to risks including virus attacks, compromise of network systems and services, and legal issues.
Target audience	This policy applies to all UNFPA personnel and outsourced providers having access to UNFPA systems and data.
Risk control matrix	Control activities that are part of the process are detailed in the Risk Control Matrix within section VI of this policy.
Checklist	N/A
Effective date	5 January 2024
Revision History	N/A
Mandatory review date	5 January 2027
Policy owner unit	Information Technology Solutions Office
Approval	Link to signed approval document

INFORMATION SYSTEMS ACCEPTABLE USE POLICY

TABLE OF CONTENTS

I. Purpose

The UNFPA information security policy mandates that all personnel must respect the ethical and acceptable use of UNFPA information and associated systems and networks. The purpose of this policy is to establish the rules and practices that constitute acceptable use of Information and Communications Technology (ICT) resources and data.

ICT resources and ICT data are defined in the definitions section below.

This policy is fundamental in managing risks, promoting responsible behavior among personnel, and ensuring compliance with international/ national data protection regulations.

II. Policy

A. Conditions applicable to use of ICT resources and ICT data

1. Use of ICT resources and ICT data shall in all cases be in accordance with the provisions set out in this policy and such other administrative issuances (including but not limited to references at section IV – related documents) as may apply to them.

2. UNFPA users who become aware of any violation of the provisions of this policy shall promptly report it to the UNFPA Office of Audit and Investigation Services (OAIS).

B. Official Use

3. Authorized users shall ensure that their use of ICT resources and ICT data is consistent with their obligations as UNFPA personnel or such other obligations (including but not limited to references at section IV – related documents) as may apply to them, as the case may be.

4. Authorized users shall use their best efforts:
    a. to ensure the accuracy and integrity of any ICT data for which they are responsible;
    b. to preserve and protect ICT resources and ICT data which may be needed by UNFPA for any purpose.

5. Access to, possession of, or distribution of sensitive data shall be in accordance with all regulations, rules and administrative issuances applicable to such sensitive data.

6. Use of Artificial Intelligence (AI) such as Generative AI applications must comply with "Principles for the Ethical use of artificial intelligence in the United Nations system" (refer related documents #2).

C. Limited personal use

7. Authorized users shall be permitted limited personal use of ICT resources, provided such use:
   a. Is consistent with the highest standard of conduct for international civil servants or the applicable standard of conduct for non-staff personnel (among the uses which would clearly not meet this standard are use of ICT resources for purposes of obtaining or distributing pornography, engaging in gambling, or downloading audio, video, image, executable or other files to which a user is not legally entitled to have access or possess);
   b. Would not reasonably be expected to compromise the interests or the reputation of UNFPA;
   c. Involves minimal additional expense to UNFPA;
   d. Takes place during personal time or, if during working hours, does not significantly impinge on such working hours;
   e. Does not adversely affect the ability of the authorized user or any other authorized user to perform his or her official functions;
   f. Does not interfere with the activities or operations of UNFPA or adversely affect the performance of ICT resources.

8. When making personal use of ICT resources, authorized users shall ensure that any such use clearly indicates that it is personal and not official in nature as per the procedures section below.

9. Personal use is a privilege that may be modified or withdrawn (by Information Technology Solutions Office [ITSO]) at any time, depending on the needs of UNFPA. Authorized users shall bear full responsibility and liability in connection with their personal use of ICT resources and UNFPA shall not bear any responsibility or liability in respect thereof.

D. Prohibited activities

10. Users of ICT resources and ICT data shall not engage in any of the following actions:
    a. Creating false or misleading ICT data
    b. Making ICT resources or ICT data available to persons who have not been authorized to access them;
    c. Using ICT resources or ICT data in a manner contrary to the rights and obligations of staff members;

d. Damaging, deleting, deteriorating, altering, extending, concealing, or suppressing ICT resources or ICT data, including connecting or loading any non-ICT resources or ICT data onto any ICT resources or ICT data
e. Accessing, without authorization, ICT data or the whole or any part of an ICT resource, including electromagnetic transmissions;
f. Using ICT resources or ICT data in violation of United Nations contracts or other licensing agreements for use of such ICT resources or ICT data or in violation of international copyright law;
g. Attempting, aiding or abetting the commission of any of the activities prohibited by this section.
h. Engaging in wrongdoing (as defined in the Oversight Policy).

11. ITSO shall have the right to block or restrict access to any ICT resource or ICT data, at any time and without notice, when necessary for maintaining or restoring the technical integrity or performance thereof or for any other appropriate purpose, including prevention of any of the activities prohibited above.

E. Monitoring and investigations

12. All use of ICT resources and ICT data may be subject to investigation by UNFPA's Office of Audit and Investigation Services (OAIS) and/or monitoring by ITSO.

III. Procedures

A. Personal use

13. Personal use of UNFPA email resources shall be indicated by including a disclaimer with the words 'personal use' at the top of emails.

14. The personal use privilege may be modified or withdrawn through notification issued by Director ITSO or through a revision of this policy.

B. Prohibited activities

15. ITSO may block or restrict access to ICT resources either by revoking access permissions or applying technical access controls to ICT resources.

C. Monitoring and investigations

16. UNFPA has a zero-tolerance principle for wrongdoing (including proscribed practices) Any violation of the provisions of this policy, shall be reported to OAIS in accordance with UNFPA Policy against Fraudulent and other Proscribed Practices.or other relevant policy that is specific to the wrongdoing.

17. Routine technical monitoring of the use of ICT resources may be conducted by ITSO or a field office focal point designated by ITSO.

18. Non-routine monitoring may be initiated by ITSO if, at any time, there is reason to believe that there has been or risk there will be use of ICT resources which significantly interferes with or impacts the operations of UNFPA.

D. Exceptions

19. Exceptions to this policy shall be managed as such:

a. Any deviation from information security policies shall be documented and submitted for review by the Information security officer via the email infosec@unfpa.org.
b. Approval of exceptions will be undertaken by the Director ITSO, in consultation with the director of the requesting entity, and documentation of approval will be retained in the central document repository.
c. Approvals to exceptions will be timebound based on the impact to organizational risk

IV. Other

A. Definitions

20. The following definitions shall apply for the purposes of the present policy:

Term	Definition
Authorized user	Any UNFPA personnel who is authorized to use information and communication technology (ICT) resources
ICT resource	any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, the United Nations Examples include but are not limited to user workstations, servers, software, cloud systems, data bases, networks, communication systems, telephones and conferencing systems.
ICT data	any data or information, regardless of its form or medium, which is or has been electronically generated by, transmitted via, received by, processed by, or represented in an ICT resource Examples include but are not limited to text, numbers, files, documents, emails, photos, and web content.
Official use	use of ICT resources by an authorized user in the discharge of his or her official functions and within the scope of his or her authorization

Personal use	use of ICT resources by an authorized user for other than official purposes and within the scope of his or her authorization;
Sensitive data	data where the unauthorized disclosure would adversely impact UNFPA operations or its reputation. It includes data whose use or distribution is otherwise restricted pursuant to UNFPA Oversight Policy.

B. Related documents

21. The following related documents should be referenced for additional context.

#	Document	Location
1	Standards of conduct for the International Civil Service	ICSC website
2	Principles for the Ethical Use of Artificial Intelligence in the United Nations System	UNCEB website
3	UNFPA General Terms and Conditions of Individual Consultant Contracts	UNFPA website
4	UNFPA policy and procedures on personal data protection	UNFPA website
5	Information disclosure policy	UNFPA website
6	Policy for UNFPA email	UNFPA website
7	Social media policy	UNFPA website
8	UNFPA website policy	UNFPA website
9	UNFPA Oversight Policy	UNFPA website
10	UNFPA Policy against Fraudulent and other Proscribed Practices	UNFPA website
11	Oversight policy	UNFPA website
12	Disciplinary framework	UNFPA website

V. Process Overview Flowchart

No overview flow chart applicable.

VI. Risk control matrix

Risk Description	First Line of Defense Controls			Second Line of Defense Controls		
	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs
UNFPA staff member utilises ICT resources for unofficial business, in a manner that impacts the availability of the resource for official business.	Policy details what level of limited personal use is permitted for UNFPA ICT resources.	Section III c	All UNFPA personnel.	Use of ICT resources shall be subject to monitoring and investigation.	Section III e	OAIS, ITSO

Risk Description	First Line of Defense Controls			Second Line of Defense Controls		
	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs	Control Activity Description	Reference (Policy section, paragraph or Control #)	Who performs
UNFPA staff member is unaware of what activities are permissible when using UNFPA ICT systems and conduct activities that detrimentally impact the reputation of UNFPA.	Policy details activities that are prohibited when using UNFPA ICT resources and ICT data.	Section III d	All UNFPA personnel.	Use of ICT resources shall be subject to monitoring and investigation.	Section III e	OAIS, ITSO
UNFPA staff member undertakes inappropriate use of ICT systems resulting in a data breach.	Policy details users' responsibility for preserving and protecting ICT resources.	Sect II b, c, d	Heads of office and line managers	Use of ICT resources shall be subject to monitoring and investigation.	Section III e	OAIS, ITSO